REMARKS

In response to the Office Action mailed on February 6, 2008, Applicant respectfully requests reconsideration. Claims 1-35, 37-40, and 42-44 are pending in this application. Claims 1-42 are rejected. Claims 36 and 41 are canceled. Claims 43 and 44 are new. Claims 1, 18, 35, 37 and 43 are independent claims, and the remaining claims are dependent claims. Applicant believes that the claims as presented are in condition for allowance. A notice to this affect is respectfully requested.

Claim Amendments

Claims 43 and 44 are new. Claim 43 claims a process that includes all of the limitations of claim 1, and includes features from claims 2, 5, and 11, and from the specification pages 3-4. Claim 44 depends on claim 43, and includes features from claim 14. Thus, no new matter has been added.

Rejections under 35 U.S.C. §103

Claims 1-13, 18-30 and 35-37 have been rejected under 35 U.S.C. §103 as being unpatentable over Weber et al. (Pub. No.: US 2006/0173992) in view of Akagawa et al. (Pub. No.: 2004/0210791). Claims 14-15 and 31-32 are rejected under 35 U.S.C. §103 as being unpatentable over Weber, in view of Akagawa, in view of Manghirmalani (USPN 5,819,028). Claims 16 and 33 are rejected under 35 U.S.C. §103 as being unpatentable over Weber, in view of Akagawa, in view of Manghirmalani, in view of Beshai et al. (Pub. No.: US 2004/0037558). Applicant traverses these rejections.

INDEPENDENT:

Claims 1, 18, 35, 36 and 37.

The office action stated that Weber discloses "receiving alert messages corresponding status events in the network, each status event having a

corresponding event category and severity value" in the Abstract, figure 10, Element-56c, and [0195]. The office action explained that "network anomalies are alert messages." This definition, however, is not accurate. Weber explicitly defines what is meant by anomalies. In paragraph [0008], Weber discloses "a device for detecting conditions in a network includes circuitry to find anomalies, which are **low-level differences in network operation** relative to some comparison period. In other words, Weber simply defines anomalies as low-level differences in network operation. Moreover, Weber does not teach **"receiving** anomalies." Instead, Weber teaches **finding** or **detecting** anomalies. This is an important difference because it demonstrates that the present invention relies on receiving input from a separate or third-party program or agent. The fact that Weber finds or detects anomalies, instead of receiving alert messages, is shown in paragraph [0006]. In this paragraph, the invention of Weber collects anomalies by traversing a connection table to identify and correlate anomalies by determining connection patterns that correlate with a particular event class. The office action also stated "anomalies is a category." This is an erroneous characterization of "anomalies." As explained, Weber defines anomalies as low-level differences in network operation. Thus, Weber fails to teach this limitation.

It is easy to understand how Weber teaches different features by considering the purpose of Weber. Weber relates to a method for preventing denial of service attacks, unauthorized access attempts, scanning attacks, and worm propagation. In other words, Weber tries to detect various attacks upon a network to protect the network. This is why Weber focuses on detecting low-level differences in network operation in an attempt to prevent denial of service attacks.

The office action stated that Weber discloses "aggregating the alert messages according to event category and severity value to generate a category specific severity ranking of the alert messages," in the Abstract. Weber, however, teaches aggregating anomalies. As explained above, anomalies are not alert messages.

The office action stated that Weber discloses "displaying a status array having a plurality of chart entries, each chart entry corresponding to alert messages of a particular event category and each chart entry having a node entry for each node having status attributable to the alert messages," in figure 29 and paragraph [0195]. Weber appears to disclose a status array having several entries, however, Weber fails to disclose that each chart entry corresponds to alert messages of a particular event category with each chart entry having a node entry for each node having status attributable to the alert messages. Instead, Weber discloses a status array showing the severity of various attacks, such as denial of service attacks, and worm propagation.

The office action stated that Weber discloses "displaying, within at least one chart entry, node entries having a status event associated with the event category for that chart entry, the node entries displayed in the chart entry according to the severity ranking and each node entry indicative of a severity scale of status for the corresponding effected node," Weber fails to completely disclose this feature. Weber discloses severity rankings for nodes indicating a status of the corresponding effected node. Weber fails to disclose node entries associated with event categories displayed in a chart entry according to a severity ranking. Thus Weber fails to disclose this feature.

DEPENDENT:

Each of the dependant claims incorporates all the limitations of its respective independent claim. As explained above, all of the independent claims are patentable over the reference combination. Therefore, all of the dependent claims are likewise patentable over the reference combination for applicable reasons as discussed above. Several of the dependent claims are further patentable over the reference combination.

Claims 2 and 19.

The office action states that Weber discloses "wherein the severity scale for a node entry is an enumeration of events received for each of the plurality of severity levels within the severity ranking," at figure 29, figure 30, and in paragraph [0195]. Weber discloses severity scales. In figure 29, network activity entries are listed with the severity column indicating a percentage and parenthetically indicating a severity level as one of low, medium, or high. The severity scale in Weber, however, is not an enumeration of events received for each of a plurality of severity levels within the severity ranking. The specification and figures of Weber are silent on this feature. In paragraph [0195], Weber explains: "The severity is determined based on what percentage of an established threshold for issuing an event notification is reached by the event. The type of event can be any of the types of events monitored by the system 10 and can include event types such as 'worm propagation', 'unauthorized access', 'DDoS attack' 'historical anomaly' and so forth." Therefore claims two and 19 are further patentable over the reference combination and believed to be allowable.

Claims 3 and 20.

The office action states that Weber discloses "the enumeration is a histogram having a magnitude based on the severity scale and a quantity of events within each security level within the severity ranking," at figure 29, in paragraph [0195]. As explained above, Weber fails to disclose that severity scale is an enumeration of events received for each of the plurality of severity levels. Weber discloses a histogram, however the histogram of Weber is an indication of traffic by IP address. Therefore, claims 3 and 20 are further patentable over the reference combination.

Claims 4 and 21.

For the rejection of these claims, the examiner took official notice that histograms can be displayed in many different shapes and colors. The examiner is correct that histograms can have many shapes and colors. Claims 4 and 20

are at least patentable over the reference combination because the independent claims from which they depend are patentable over the reference combination as discussed above.

Claims 11 and 28.

The office action states that Weber discloses "processing and propagating the threshold values to remote agents, the remote agents operable to analyze nodes and determine when a particular metric satisfying a triggering threshold is attained and generate the corresponding event," in the Abstract. Weber does not disclose this feature. In the Abstract, Weber discloses "collector devices." In paragraph [0045], Weber explains "the collector devices 12 collect information such as source and destination addresses, transport protocol, source and destination ports, flags, and length. Periodically, the collector devices 12 send to the aggregator 14 a record of the number of packets, bytes, and connections between every host pair observed by the collector 12, broken down by port and protocol." In other words, the collectors of Weber simply collect information and forward this information to the invention of Weber. Weber, however, is completely silent on propagating threshold values to remote agents.

Claims 38-42.

Claim 38 claims "the severity scale for each node entry is an aggregate value representative of a number of alert messages received at each node entry for a given sampling interval." Weber is silent on the severity scale being an aggregate value of a number of alert messages. As discussed above, Weber at least fails to disclose alert messages.

Claims 16 and 33.

Claims 16 and 33 are patentable over the reference combination because their parent claims are patentable over Weber. Claims 16 and 33 are further patentable over the reference combination because Beshai was erroneously

combined with Weber, Akagawa, and Manghirmalani. There is no motivation to combine Beshai in the reference combination. Beshai relates to a modular optical switch, and focuses on receiving optical signals from, and transmitting optical signals to, edge nodes. Beshai also relates to time-sharing schemes, and path selections. Therefore claims 16 and 33 are further patentable over the reference combination.

Claims 43 and 44

Claims 43 and 44 are new. Claim 43 is independent and claim 44 depends on claim 43. Claim 43 further clarifies at least one distinguishing feature of the Applicant's invention. Applicant notes that claim 43 includes the limitation:

> "propagating threshold values to remote agents, wherein responsive to the threshold values, the remote agents operable to analyze nodes and determine when a particular metric satisfying a triggering threshold is attained, and to generate a corresponding status event as an alert message;
> receiving alert messages, from the remote agents, corresponding to status events in the storage area network, each status event having a corresponding event category and severity value."

This feature is described in the specification page 6 lines 11-17, and in claim 11. Weber is silent on propagating thresholds to agents/collectors. As described in paragraph [0048] of Weber, collectors transmit statistics (bytes/second, packets/second, connections/hour) to a central aggregator. The aggregator then groups, processes and analyzes data to identify anomalies in network activity to find DoS attacks. The remaining features of claim 43, such as, for example, "the severity scale for a node entry is an enumeration of events received for each of a plurality of severity levels with the severity ranking" is patentable over the reference combination as described above. Therefore claims 43 and 44 are believed to be allowable.

Summary

The claims are patentable over the reference combinations because the combined references fail to teach all of the features of the claimed invention. Therefore the claims are believed to be in condition for allowance.

Applicant hereby petitions for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

Respectfully submitted,

/joshuadmather/

Joshua D. Mather
Attorney for Applicant(s)
Registration No.: 53,282
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: EMC03-12(02169)

Dated: July 7, 2008